一种适用于分布式审批工作流的多重短签名方案 *

左黎明 [a, b]，陈兰兰 [a, b]，周 庆 [a, b]

(华东交通大学 a. 理学院, b. 系统工程与密码学研究所, 南昌 330013)

摘 要：传统单路线性工作流难以满足高并发、时效性高的管理事务需求，而采用多层网状分布式架构可以有效解决此类问题。针对分布式审批工作流业务系统中存在的数据交互安全问题，提出了一种安全性较高、签名长度较短的多重短签名方案。首先，在随机预言机模型和 CDH 困难问题假设下，证明了签名方案的安全性；基于此方案设计了分布式审批工作流交互协议，并进行了安全性分析；运用 C 语言实现了签名方案，并与同类签名方案进行了效率比较；最后对基于此签名方案的应用系统的优势进行了分析。结果表明，该签名方案效率较高、计算量小，因此，基于此方案的分布式审批工作流适用于高并发、时效性要求高的电子政务系统。

关键词：分布式架构；工作流；多重短签名；协议

中图分类号：TP309.2 doi: 10.19734/j.issn.1001-3695.2018.07.0561

Short multi-signature scheme for distributed approval workflow

Zuo Liming[1, 2], Chen Lanlan[1, 2], Zhou Qing[1, 2]

(*a. School of Science, b. SEC Institute, East China Jiaotong University, Nanchang* 330013, *China*)

Abstract: Traditional single-route workflows are difficult to meet the high concurrency and time-sensitive management transaction requirements, and multi-layer mesh distributed architecture can effectively solve such problems. Aiming at the problem of data interaction security in the distributed approval workflow business system, this paper proposed a short multi-signature scheme suitable for distributed approval workflow with high security and short signature length. It firstly proved the security of the signature scheme under the random oracle model and the assumption of CDH difficult problem. Then, it designed a distributed approval workflow interaction protocol based on the scheme and carried out the security analysis. It implemented the signature scheme by C language and compared the proposed signature scheme with some similar signature schemes. Finally, the paper analyzed the advantages of the application system based on this signature scheme. The results show that the signature scheme proposed has high efficiency and small amount of calculation. Therefore, the distributed approval workflow based on the scheme is suitable for e-government systems with the demands of high concurrency and time effectiveness.

Key words: distributed architecture; workflow; short multi-signature; protocol

0 引言

传统的工作流技术面向集中式应用，但随着现代企业规模的日趋扩大，信息呈现出一种分布、异构、松散耦合的状态，传统的工作流技术已无法满足海量数据下的信息管理需求。尤其对于面向政府机关的电子政务系统，管理事务繁琐、需要层层审批，在高并发、时效性要求高的环境下，传统工作流难以满足此类系统需求，而采用多层网状的分布式架构可以有效地解决此类问题。2018 年，Pan[1]对分布式工作流管理系统的代理根据其功能进行划分，并对代理的每种类型的执行过程进行分析，对流程执行和资源管理等关键技术进行了研究与实现。但 Pan 对分布式工作流的技术研究主要关注于其功能，很少提及对审批信息的安全性保护。对于面向政府机关内部以及其他政府机构的系统，信息的保密至关重要。因此，将数字签名应用于分布式审批工作流中，构造一种适用于分布式审批工作流的多重短签名方案，对审批信息进行保护，对采用分布式审批工作流的业务系统的数据安全性而言具有重要意义。

多重签名（multi-signature, MS）的概念由 Itakura 等人[2]于 1983 年首次提出，是一种多个用户对同一消息的特殊签名，适用于一个文件需要多个人同时签名的场景，比如逐层审批的文件，在电子商务、电子政务等领域具有广泛的应用。近年来，国内外许多专家学者对多重签名方案进行构造与改进。2015 年，Sahu 等人[3]提出了采用双线性对的基于身份的多代理多重签名方案，并在计算 Diffie-Ellman 假设和随机预言模型下证明其在自适应选择身份攻击下是抗存在伪造的。2016 年，杜红珍[4]采用双线性对技术构造了一种高效的基于身份的有序多重签名机制，并在计算性 Diffie-Hellman 困难假设下证明了其在适应性选择消息和身份攻击下是抗存在性伪造。2017 年，Pankaj 等人[5]提出了一种采用双线性对的基于身份的多代理多重签名方案，并证明该方案具有较高的效率和安全性。还有一些学者相继提出其他多重签名方案[6~9]。但上述大部分签名方案签名长度较长，在网络条件较差的环境下，存在签名传输、存储效率较低等问题。因此，构造一种签名长度较短、安全性较高的多重签名具有重要意义。

短签名的概念由 Boneh 等人[10]首次提出，其签名长度是 DSA 签名长度的一半，具有更高的签名效率。本文将短签名引入多重签名，构造了一种适用于分布式审批工作流的多重

收稿日期：2018-07-18；**修回日期：**2018-09-06 **基金项目：**国家自然科学基金资助项目（11761033）；江西省教育厅科技项目（GJJ161417, GJJ170386）

作者简介：作者名：左黎明（1981-），男，江西鹰潭人，副教授，硕士，主要研究方向为信息安全、非线性系统（limingzuo@126.com）；陈兰兰（1995-），女，江西九江人，硕士研究生，主要研究方向为信息安全；周庆（1993-），男，江西宜春人，硕士研究生，主要研究方向为信息安全.

短签名方案，该方案具有签名长度短、安全性高的优势。并设计了相应的交互协议，适用于需要逐层审批的电子政务系统，并且满足安全性高、数据量大、高并发、松耦合的事务管理需求。

1　安全的分布式审批工作流原理

如图 1 所示，本文论述的安全的分布式审批工作流的业务系统需要有密钥生成中心（key generation centre，KGC）和审批网络。审批网络结构如图 2 所示，主要包括信息提交用户 *User*、信息接收节点 *Start*、退回节点 *Fail*、审批完成节点 *End*、信息处理节点 *Info* 以及 M 个审批层 A_i $(1\le i\le M)$，其中每个审批层中包含若干个审批节点 $U_{i,j}$ $(1\le i\le M,\ 1\le j\le N_i)$。令 $U_i\in\{U_{i,1},U_{i,2},\cdots,U_{i,N_i}\}$ $(i=1,2,\cdots,M)$，即从每个审批层中选取一个审批节点，则选取的 M 个审批节点 $U_1,U_2,\cdots,U_M$ 与节点 *Start* 以及 *End* 构成一条审批链 L，审批链中的每个节点选取规则是选择每个审批层中当前队列最短的审批节点，且一条审批链完成一轮工作流审批。具体参数说明如表 1 所示。

表 1　参数列表

Tab 1 Parameters list

序号	参数名	说明
1	*User*	信息提交用户
2	*Start*	信息接收节点
3	*Fail*	退回节点
4	*End*	审批完成节点
5	*Info*	信息处理节点
6	A_i	审批层
7	$U_{i,j}$	审批节点
8	U_i	选取的审批节点
9	L	审批链

审批工作流要件具体说明如下：

a）密钥生成中心，主要工作是为审批网络中每个审批节点产生并分配密钥对。由于用户提交的待审批信息具有私密性，密钥生成中心需要对审批过程进行全程监控，故系统需求分析上有一些特殊要求：①仅密钥生成中心可验证，在获得密钥生成中心授权情况下被授权者也可验证；②利用密钥生成中心主密钥和审批节点索引号即可进行安全认证。

b）审批网络。如图 2 所示，审批网络包括若干条审批链，对于一条审批链 $L=\{Start,U_1,U_2,\cdots,U_M,End\}$，信息提交用户提交信息给信息接收节点 *Start*，节点 *Start* 将信息封装后，发送给审批链 L 的第一个审批节点 U_1。U_1 先审批信息，如果不满足审批要求，则将退回结果和信息发送给退回节点 *Fail*，否则对信息进行签名，并发送给下一个审批节点 U_2。U_2 先验证签名的有效性，如果无效，则将无效结果和信息直接退回到节点 *Fail*；如果有效则开始审批信息，若不满足审批要求，则将退回结果和信息发送给节点 *Fail*，否则对信息进行签名，并发送给下一个审批节点。直到最后一个审批节点 U_M 接收信息，先验证签名的有效性，如果无效，则将无效结果和信息直接退回到节点 *Fail*；如果有效则开始审批信息，若不满足审批要求，则将退回结果和信息发送给节点 *Fail*，否则对审批通过结果和信息进行签名，将签名发送给审批完成节点 *End*。至此，一条审批链审批工作流结束。节点 *Fail* 和 *End* 最终将审批结果发送给信息处理节点 *Info*，节点 *Info* 再将审批结果返回给信息提交用户。

根据以上系统原理与需求，本文设计了一种适用于分布式审批工作流的多重短签名方案，以此来提高工作流系统的安全性，而设计一种安全高效的多重短签名方案是关键。

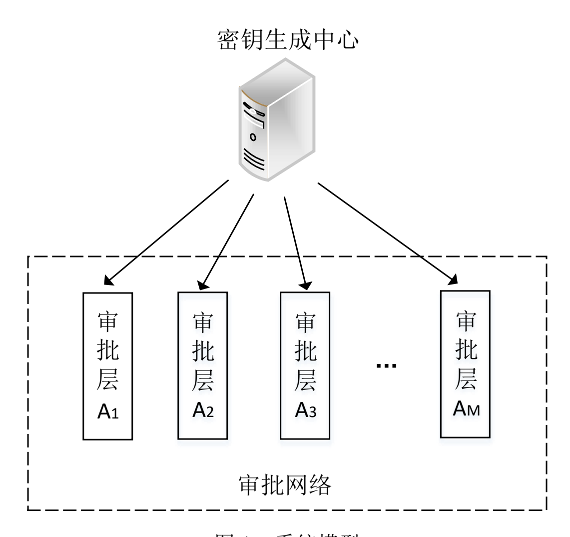


图 1　系统模型

Fig. 1　System model

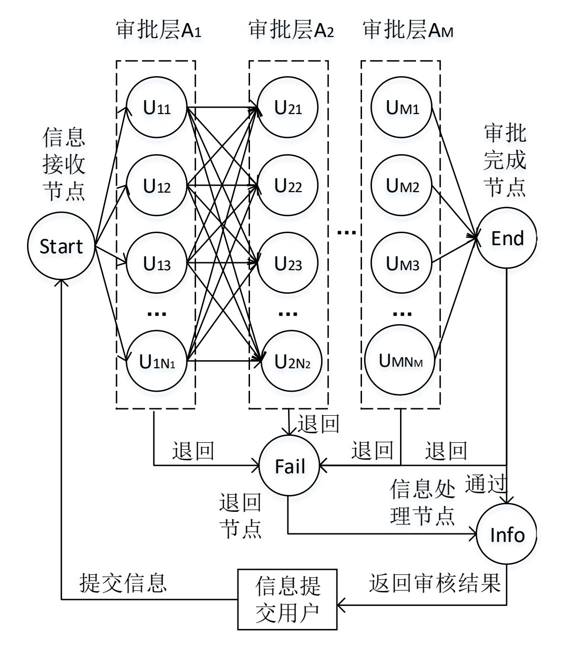


图 2　审批网络结构

Fig. 2　Approval network structure

2　多重短签名方案设计与安全性分析

2.1　数学基础

定义 1　计算性 Diffie-Hellman 问题(computational Diffie-Hellman, CDH)。给定 $P,aP,bP\in G_1$（$a,b\in Z_q^*$ 是未知的随机数），计算 $abP\in G_1$ 是困难的。

定义 2　双线性对（bilinear pairings）。给定一个安全参数 k，G_1 为 q 阶循环加法群，G_2 为同阶循环乘法群，其中 P 为 G_1 的生成元，q 为一个 $k-bit$ 素数，则称映射 $e:G_1\times G_1\to G_2$ 为双线性对，如果满足以下三条性质：

a)双线性性，对 $\forall a,b\in Z_q^*$，有 $e(aP,bP)=e(P,P)^{ab}$；

b)非退化性，$e(P,P)\ne 1$；

c)易计算性，$\forall Q,R\in G_1$，存在有效算法计算 $e(Q,R)$。

2.2　多重短签名方案

一般多重短签名的方案定义如文献[4]中所述，根据前述对安全审批工作流的需求分析要求，本文构造了一种适用于分布式审批工作流的多重短签名方案。方案由系统初始化、审批节点密钥生成与注入、审批链与多重签名、多重签名验

证以及授权签名验证五个高效算法组成，具体过程如下：

a)系统初始化。密钥生成中心KGC给定一个安全参数 k ，选择一个大素数 q ， G_1 、 G_2 为 q 阶循环群， P 为 G_1 的生成元。选择一个安全的双线性映射 $e:G_1 \times G_1 \to G_2$ 。KGC 随机选择 $s \in Z_q^*$ 作为系统主密钥，并计算 $P_{pub}=sP$ 作为主公钥。选择安全的 Hash 函数 $H_1:\{0,1\}^* \to Z_q^*$ ， $H_2:\{0,1\}^* \to G_1$ ，则 KGC 公布系统参数 $params=\{q,P,e, G_1,G_2,P_{pub},H_1,H_2\}$ ，KGC 掌握系统主密钥 s 。

b)审批节点密钥生成与注入。在连接审批网络前，每个审批层的每个节点需要在 KGC 登记。每个审批节点输入身份 ID ，KGC 随机选择一个密钥生成标记 $K_{ID} \in Z_q^*$ ，生成审批节点私钥 $x_{ID}=sH_1(ID,K_{ID},s)$ ，并秘密保存 K_{ID} ，计算公钥 $y_{ID}=x_{ID}P$ 。密钥生成中心通过身份 ID 建立索引对审批节点的信息进行管理，不同身份的审批节点使用不同的密钥生成标记，并通过安全方式向身份 ID 的审批节点注入密钥。这种密钥生成的方式与已有的数字签名方案均有不同，是为了实现前述特殊要求的①和②。

c) 审批链与多重签名。对于一条审批链 $L=\{Start,U_1,U_2,\cdots,U_M,End\}$ ，用户提交待审批信息到信息接收节点 $Start$ ，如果该信息符合所有审批条件，则会执行到审批通过节点 End ，否则，退回到退回节点 $Fail$ 。审批链对提交的待审批信息 $m \in \{0,1\}^*$ 具体审批步骤如下：

(a) $Start$ 具体操作过程如下：设 T 为 $Start$ 收到信息 m 的时间，用于记录消息初次进入审批队列时间。将消息 m 和时间 T 发送给第一个审批节点 U_1 。

(b) U_1 收到信息后操作过程如下：计算 $h=H_2(m,T)$ ， $S_1=ID_1x_{ID_1}h$ ，将部分签名 S_1 、身份 ID_1 、信息 m 以及 T 发送给下一个审批节点 U_2 。

(c) U_2 首先验证 S_1 的有效性，再附加签名，具体过程如下：

i) 计算 $h=H_2(m,T)$ ；

ii) 验证 $e(S_1,P)=e(h,ID_1y_{ID_1})$ 是否成立，如果不成立，则将信息 m 发送给退回节点 $Fail$ 并结束审批，否则 U_2 继续审批；

iii) 计算 $S_2=S_1+ID_2x_{ID_2}h$ ，将部分签名 S_2 ，身份 ID_1 ， ID_2 ，信息 m 以及 T 发送给下一个审批节点 U_3 。

(d) U_i $(i=3,4,\cdots,M)$ 收到第 $i-1$ 个审批节点 U_{i-1} 发送的部分签名 S_{i-1} ，身份 ID_1 ， ID_2 ，…， ID_{i-1} ，信息 m 以及 T 后，首先验证 S_{i-1} 的有效性，再附加签名，具体过程如下：

i) 计算 $h=H_2(m,T)$ ；

ii) 验证 $e(S_{i-1},P)=e(h,\sum_{j=1}^{i-1}ID_jy_{ID_j})$ 是否成立，如果不成立，则将信息 m 发送给退回节点 $Fail$ 并结束审批，否则 U_i 继续审批；

iii) 计算 $S_i=S_{i-1}+ID_ix_{ID_i}h$ ，则 S_i 为 i 个审批节点 $U_1,U_2,\cdots,U_i$ 对信息 m 的部分签名。当 $i=M$ 时，得到的签名 S_M 为审批链 L 中 M 个审批节点 $U_1,U_2,\cdots,U_M$ 对信息 m 的多重短签名。

最后，审批节点 U_M 将签名 S_M ，身份 ID_1 ， ID_2 ，…， ID_M ，信息 m 以及 T 发送给审批通过节点 End 。

d) 多重签名验证。审批通过节点 End 验证 $e(S_M,P)=e(h,\sum_{i=1}^{M}ID_iy_i)$ 是否成立，如果成立，则签名有效，将审批通过结果发送给 $Info$ ；否则签名无效，退回到 $Fail$ ， $Fail$ 再将审批失败结果发送给 $Info$ 。$Info$ 最终将审批结果进行处理并返回给用户。签名算法正确性验证如下：

$$e(S_M,P)=e(\sum_{i=1}^{M}ID_ix_{ID_i}h,P)\ =e(h,\sum_{i=1}^{M}ID_iy_{ID_i})$$

e)授权签名验证。密钥生成中心向验证者公开身份为 ID_i 的审批节点对应的授权信息 $Q_i=H_1(ID_i,K_{ID_i},s)$ ，任何人都可以通过审批节点的身份 ID 和 Q 验证签名的有效性。验证等式

$$e(S_M,P)\ =e(H_2(m,T),\sum_{i=1}^{M}ID_iQ_iP_{pub})$$

是否成立，如果成立，则签名有效，确认审批通过，否则签名无效，确认审批失败。

2.3 安全模型与安全性分析

定义 3 敌手 A(签名攻击算法)和挑战者 C 之间的攻击游戏交互过程如图 3 所示，如果伪造的签名 S_n^* 满足存在一个 $\hat{m}$ 没有做过多重签名询问条件，并在验证算法中验证有效，则称 A 在游戏中获胜。

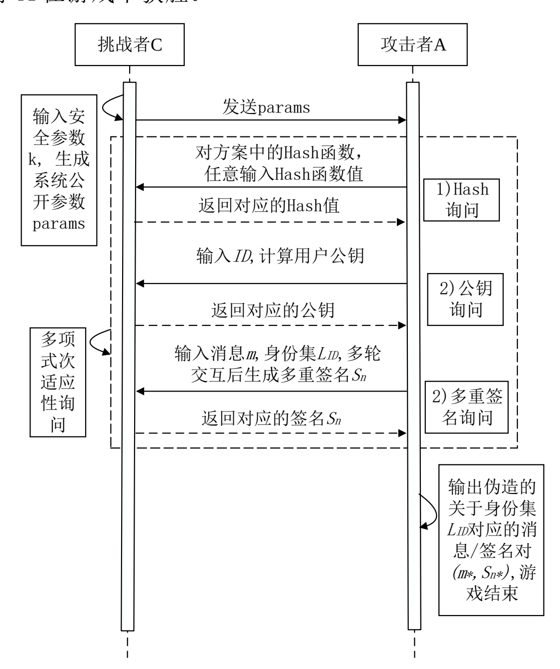


图 3　攻击游戏交互过程

Fig. 3　Attack game interaction process

如果不存在概率多项式签名攻击算法 A 在如图 3 游戏中获胜，则称该方案在适应性选择消息下抗存在性伪造攻击。

定理 1 在随机预言机模型和 CDH 困难问题假设下，本文提出的多重短签名方案在适应性选择消息攻击下是抗存在性伪造的。

引理 1 假设存在敌手 A 在概率多项式时间 t 内以不可忽略的概率 ε 攻破本文方案，记 $H_i(i=1,2)$ 预言机询问、公钥询问和多重签名询问次数分别为 q_{H_i} $(i=1,2)$ 、 q_K 和 q_S ，一次询问所需时间分别为 t_{H_i} 、 t_K 和 t_S ， $\delta \in (0,\frac{1}{2})$ ，则存在算法 C，在时间：

$$t'<t+(q_St_S+q_Kt_K+2q_{H_1}t_{H_1}+2q_{H_2}t_{H_2})$$

内以不可忽略的优势： $\varepsilon' \ge (\varepsilon-\frac{1}{2^k})\delta(1-\delta)^{q_S}$ 解决 CDH 问题。

证明 设挑战者 C 挑战的 CDH 问题实例为：给定 $P,aP,bP \in G_1$ （ $a,b \in Z_q^*$ 未知），计算 $abP \in G_1$ 。C 要借助 A 的能力求解困难问题实例。

设安全参数为 k ，C 运行系统初始化算法，将 aP 作为系统主公钥 P_{pub} 的值，生成系统参数 $params=\{q,P,e, G_1,G_2,P_{pub},H_1, H_2\}$ ，将 $params$ 发送给 A。为了方便后面的签名伪造，C 维护一个特定的消息集 Ω ，并初始化为空。假设 A 在签名询问前都已做过相应的 H_1 询问和 H_2 询问等前置询问，所有记录列表初始化置为空。

a) H_1 询问。C 维护一个列表 L_{H_1}，记存储结构为数组 (ID_i, K_{ID_i}, r_i)。当 A 输入 (ID, K_{ID}) 进行 H_1 预言机询问时，C 查询 L_{H_1} 中是否存在对应的记录 (ID, K_{ID}, r)，如果存在，则返回相应值 r 给 A，否则 C 随机选择一个 $r \in Z_q^*$，将 r 返回给 A，并将 (ID, K_{ID}, r) 记录到列表 L_{H_1} 中。

b)公钥询问。C 维护一个列表 L_K，记存储结构为数组 (ID_i, r_i, y_i)。当 A 输入 ID 进行公钥询问时，C 查询 L_K 中是否存在对应的记录 (ID, r, y)，如果存在，则返回相应的公钥 y 给 A，否则先做 H_1 询问获得 r，计算公钥 $y = raP$ 返回给 A，同时将 (ID, r, y) 添加到列表 L_K 中。

c) H_2 询问。C 维护一个列表 L_{H_2}，记存储结构为数组 (m_i, T_i, t_i, h_i)。A 输入 (m, T) 进行 H_2 询问时，C 查询 L_{H_2} 中是否已经存在对应的记录 (m, T, t, h)，如果存在，则返回其中相应值 h 给 A，否则：

(a)C 以 δ 的概率随机选择一个 $t \in Z_q^*$，将 tbP 返回给 A，并将 $(m, T, t, h = tbP)$ 记录到 L_{H_2} 中，并将 m 添加到消息集 Ω 中；

(b)C 以 $1-\delta$ 的概率随机选择一个 $t \in Z_q^*$，将 tP 返回给 A，并将 $(m, T, t, h = tP)$ 记录到 L_{H_2} 中。

d)多重签名询问。A 输入消息 m、时间 T 以及 $ID_1, ID_2, \cdots, ID_{j-1}$ 上的部分签名 S_{j-1}，进行关于身份 ID_j $(2 \le j \le M)$ 的部分签名询问：

(a)如果 $m \in \Omega$，C 挑战失败，并输出“FAILURE”(记此事件为 E_1 事件)；

(b)如果 $m \notin \Omega$，C 从列表 L_{H_1} 中获得对应的记录 (ID_j, K_{ID_j}, r_j)，从列表 L_{H_2} 中获得对应的记录 $(ID_j, m, T, t_j, h_j = t_j P)$，计算 $S_j = S_{j-1} + ID_j r_j t_j aP$，C 把 S_j 作为对消息 m 的部分签名，并将 S_j 返回给 A。

经过多项有界式次适应性询问后，A 停止询问并输出一个关于消息 m^* 和有序身份集 $L_{ID}^* = \{ID_1^*, ID_2^*, \cdots ID_M^*\}$ 的有效多重签名 S_M^*。

(a)如果 $m^* \notin \Omega$，则 C 挑战失败，并输出“FAILURE”，(记此事件为 E_2 事件)；

(b)如果 $m^* \in \Omega$，则 C 从列表 L_K 中获取记录 (ID_i^*, r_i^*, y_i^*) $(1 \le i \le M)$，从列表 L_{H_2} 中获取记录 (m^*, T^*, t^*, h^*)，此时 $h^* = t^* bP$，从而有

$$e(S_M^*, P) = e(h^*, \sum_{i=1}^{M} ID_i^* y_i^*)$$
$$= e(t^* bP, \sum_{i=1}^{M} ID_i^* r_i^* aP)$$
$$= e(\sum_{i=1}^{M} ID_i^* r_i^* t^* abP, P),$$

因此 C 可以成功计算出：

$$abP = (\sum_{i=1}^{M} ID_i^* r_i^* t^*)^{-1} S_M^*,$$

所以 C 输出 $(\sum_{i=1}^{M} ID_i^* r_i^* t^*)^{-1} S_M^*$ 作为 CDH 困难问题实例的一个解。下面分析 C 成功解决困难问题的时间和优势：

(a)对 H_1 和 H_2 询问的每个应答在 Z_q^* 和 G_1 中是均匀分布的，且应答都是有效的;

(b)只有当询问阶段事件 E_1 一直不发生和签名伪造阶段 E_2 也不发生时，多重签名询问的应答才是有效的。事件 E_1 不发生的概率满足：$P(\neg E_1) \ge (1-\delta)^{q_S}$，事件 E_2 不发生的概率满足：$P(\neg E_2) \ge \delta$。然而，如果 A 没有询问 H_2 就伪造了一个有效签名，这种模拟就存在缺陷，其发生概率为 $\frac{1}{2^k}$，所以 C 成功求解困难问题实例的优势满足：

$$\varepsilon' \ge (\varepsilon - \frac{1}{2^k})\delta(1-\delta)^{q_S},$$

时间限满足：

$$t' < t + (q_S t_S + q_K t_K + 2q_{H_1} t_{H_1} + 2q_{H_2} t_{H_2})。$$

因此 C 以不可忽略的优势 ε' 在多项式时间 t' 内成功的解决了一个 CDH 问题的实例，这与 CDH 问题困难性矛盾。所以本文方案是存在性不可伪造的。因此定理 1 得证。

3　应用协议设计与安全性分析

3.1　协议设计

传统的审批工作流为单路线性工作流，不适合在高并发和时效性要求高的场合，尤其是某些需要多部门配合层层审批的电子政务系统，而采用多层网状分布式架构能有效地解决此类问题，但跨多个服务器可能存在审批流程出现安全问题。利用本文方案可以构造了一个安全的分布式审批工作流协议。具体协议交互过程如下：

(1) $User \rightarrow Start$：m；

(2) $Start \rightarrow U_1$：m, T；

(3) $U_1 \rightarrow U_2$：S_1, ID_1, m, T, t_i；

(4) $U_{i-1} \rightarrow U_i$：$S_i, ID_1, ID_2, \cdots, ID_{i-1}, m, T, t_{i-1}$，其中 $i = 3, 4, \cdots, M$；

(5) $U_M \rightarrow End$：$S_M, ID_1, ID_2, \cdots, ID_M, m, T, t_i$；

(6) End 验证签名 S_M，若验证通过，则签名有效，将审批完成结果发送给 $Info$，否则签名无效，退回到 $Fail$，$Fail$ 再将审批失败结果发送给 $Info$；

(7) $Info \rightarrow User$：“true”或“false”。

3.2　协议交互过程的安全性分析

1)抗存在性伪造攻击

从 3.1 协议的交互过程可以看出，节点间传递是单向的，只有一次交互，协议安全性由签名方案的安全性保证。由 2.3 节签名方案安全性分析可知，本文提出的基于多重短签名的分布式工作流审批协议在适应性选择消息攻击下是抗存在性伪造的。

2)抗中间人攻击

由本文构造的多重短签名方案可知，恶意中间人攻击者若要成功伪造目标身份的签名 S_M，必须满足以下验证等式：

$$e(S_M, P) = e(h, \sum_{j=1}^{M} ID_j y_{ID_j})$$

而由 2.3 节签名方案安全性分析可知，当 $P_{pub} = ap$，$h_M^* = bP$ 时，有如下等式成立：

$$e(S_M^*, P) = e(bP, \sum_{i=1}^{M} ID_i^* r_i^* aP)$$
$$= e(\sum_{i=1}^{M} ID_i^* r_i^* abP, P)$$

此时可以计算出 $abP = (\sum_{i=1}^{M} ID_i^* r_i^* t^*)^{-1} S_M^*$，其中 S_M^* 为目标身份 ID_M^* 的伪造签名，意味着解决了 CDH 困难问题。因此恶意中间人攻击者无法伪造目标身份的签名。

3)抗消息重放攻击

在工作流审批过程中采用了时戳机制，对每次用户提交的待审批信息在初次进入审批工作流都会添加时戳 T，从而保证了信息的新鲜性。任何截取了待审批信息的攻击者都不能通过重放再次通过验证，审批链中每个审批节点会重新对时戳进行验证，若验证有效，则接受签名，否则将信息退回并拒绝继续签名。

4　签名方案实现与效率分析

4.1　方案实现

本文在 windows7 64 位操作系统的 Microsoft Visual Studio 2012 开发平台下，采用 C 语言实现本文签名方案，实现结果如图 4 所示，方案核心代码如下：

```
//3.审批链与多重签名
//计算 h=H2(m,T)
element_from_hash(h,m,strlen(m));
//用户 1 部分签名
element_mul(data1,ID1,X1);
element_mul(S1,data1,h);
//用户 2 验证
element_pairing(left1,S1,P);//等式左边
element_mul(temp1,ID1,Y1);//ID1*Y1
element_pairing(right1,h,temp1);//等式右边 e(h,ID1*Y1)
// 左右比较
if (element_cmp(right1, left1))
  printf("用户 1 签名无效！ \n");//左右不同
else{
  printf("用户 1 签名有效！ \n");//左右相同
  //用户 2 部分签名
  element_mul(data1,ID2,X2);
  element_mul(temp4,data1,h);
  element_add(S2,S1,temp4);
  //用户 3 验证
  element_pairing(left1,S2,P);// e(S2,P)
  element_mul(temp2,ID2,Y2);//ID2*Y2
  //ID1*Y1+ID2*Y2
  element_add(temp3,temp1,temp2);
  element_pairing(right1,h,temp3);
  // 左右比较
  if (element_cmp(right1, left1))
    printf("用户 2 签名无效！ \n");
  else{
    printf("用户 2 签名有效！ \n");//相同
    //用户 3 签名，S3 为最终多重签名
    element_mul(data1,ID3,X3);
    element_mul(temp5,data1,h);
    element_add(S3,S2,temp5);
    //4.多重签名验证
    element_pairing(left1,S3,P);// e(S3,P)
    element_mul(temp5,ID3,Y3);//ID3*Y3
    element_add(temp6,temp3,temp5);
   element_pairing(right1,h,temp6);
  }
}
```

4.2　效率分析

通过查阅文献，其他学者关于多重短签名方案的研究很少，因此本文只与其他多重签名方案进行效率分析。表 2 为本文方案与其他多重签名方案在签名和验证阶段的比较，其中 P 表示双线性对运算，M 表示标量乘运算，E 表示指数运算。

由表 2 可见，本文方案在签名阶段需要 2 次标量乘运算，验证阶段需要 1 次标量乘运算和 2 次双线性对运算。与文献[12]方案相比，计算量较接近，与文献[5,11]方案相比，本文无论在计算性能和签名长度上都有优势。



图 4　方案实现结果

Fig. 4　Scheme implementation results

表 2　多重签名方案效率比较

Tab 2 Efficiency comparison of multi signature schemes

方案	签名	验证	签名长度
文献[5]方案	$4M$	$4P+2E$	320
文献[11]方案	$3M+1E$	$3P+1E$	320
文献[12]方案	$2E$	$2E$	2208
本文方案	$2M$	$1M+2P$	160

5　基于多重短签名方案的系统应用优势分析

5.1　系统整体安全性优势分析

一般分布式工作流系统可以满足高并发、时效性要求高的事务管理需求，但往往需要跨多个服务器运行，数据在传输时面临着数据伪造、抵赖、冒充和窜改等信息安全问题，而基于多重短签名方案的分布式工作流系统能有效避免这些问题。多重短签名方案适用于多个用户对同一消息签名的场景，基于该签名方案，分布式工作流系统审批网络中每条审批链的每个审批节点在接收到信息后，都可以对信息的有效性进行验证，从而大大提高数据来源的可靠性和数据传输的完整性，防止审批节点否认与伪造信息。

5.2　签名性能优势分析

本文提出的基于多重短签名方案，其签名长度减少到 160 bit，是 DSA 签名长度的一半，且具有高效的计算效率，在网络状态较差、网络传输不稳定的条件下具有良好的适用性。在移动网络环境下，对于一个长度为 1480 Byte 的消息，短签名长度为 20 Byte，而普通签名则需 40 Byte，交互 1 次可以节省 20 Byte 流量。而通信过程中一次传输所能通过的最大数据包大小有限，由于缩短了签名长度，每次交互可以携带更多的业务信息，从而避免因数据量大被分片而导致通信效率降低，因此对事务繁琐、交互频繁的业务系统具有明显的优势。

6　结束语

本文提出了一种适用于分布式审批工作流的多重短签名方案，并设计了适用的安全交互协议。在 CDH 困难问题假设和随机预言机模型下，证明了签名方案在适应性选择消息下是抗存在性伪造的，同时实现了签名方案，并进行了效率

分析。该方案适用于需要逐层审批的电子政务系统，采用多层网状分布式架构，满足高并发和时效性高的业务需求，同时签名方案又具有较高的安全性，使系统可以安全高效地运行。

参考文献：

[1] Pan Tianheng. Research and implementation of key technologies in multi-agent system to support distributed workflow [C]//IOP Conference Series: Earth and Environmental Science, 2018.

[2] Itakura K, Nakamura K. A public-key cryptosystem suitable for digital multisignatures [J]. NEC Research & Development, 1983(71): 1-8.

[3] Sahu R A, Padhye S. Identity-based multi-proxy multi-signaure scheme provably secure in random oracle model [J]. Transactions on Emerging Telecommunications Technologies, 2015, 26(4): 547-558.

[4] 杜红珍. 适于车载网的安全高效的有序多重签名机制 [J]. 计算机应用研究, 2016, 33(10): 3105-3108. (Du Hongzhen. Secure and efficient sequential multisignature scheme for VANET [J].Application Research of Computers, 2016, 33(10): 3105-3108.)

[5] Sarde P, Banerjee A, Dewangan C L. A secure and an efficient ID-based multi-proxy multi-signature scheme from bilinear pairings [J]. International Journal of Computer Applications, 2017, 157(10): 1-6.

[6] Naoto Y, Eikoh C, Masahiro M, *et al*. A CDH-based ordered multisignature scheme provably secure without random oracles [J]. Journal of Information Processing, 2014, 22(2): 366-375.

[7] Wang F, Chang C C, Lin C, *et al*. Secure and efficient identity-based proxy multi-signature using cubic residues [J]. International Journal of Network Security, 2016, 18(1): 90-98.

[8] 杨青, 辛小龙, 李小光. 改进的超椭圆曲线结构化多重盲签名 [J]. 工程数学学报, 2017, 34(3): 247-261. (Yang Qing, Xin Xiaolong, Li Xiaoguang. Improved structured blind multisignature schemes based on hyperelliptic curves [J]. Chinese Journal of Engineering Mathematics, 2017, 34(3): 247-261.)

[9] Wei L, Zhang L, Huang D, *et al*. Efficient and provably secure identity-based multi-signature schemes for data aggregation in marine wireless sensor networks [C]//Proc of IEEE International Conference on Networking, Sensing and Control. IEEE, 2017: 593-598.

[10] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing [C]// Proc of the 7th International Conference on Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001: 514-532.

[11] 秦艳琳, 吴晓平. 高效的无证书有序多重签名方案 [J]. 通信学报, 2013, 34(7): 105-110. (Qin Yanlin, Wu Xiaoping. Efficient certificateless sequential multi-signature scheme [J]. Journal on Communications, 2013, 34(7): 105-110.)

[12] Wei Lifei, Cao Zhenfu, Dong Xiaolei Secure. identity-based multisignature schemes under quadratic residue assumptions [J]. Security and Communication Networks, 2013, 6(6): 689-701.